Excerpt from
Japanese Patent Laid-Open Publication No. Sho 61-246787

[Means for Solving the Problem]

Fig. 1 shows a block diagram showing the principle of the present invention. In the drawing, numeral 1 denotes a first random number generator; numeral 2 denotes a second random number generator; numeral 3 denotes a decoder which selects any one of W buffers; and numerals4-1 to 4-W denote buffers which store and output each value of the second series of random number sequence in accordance with the instructions from the decoder 3.

[Operation]

In Fig. 1, assuming that the second series of random number sequence are q-valued random numbers, random transposition which randomly distributes W buffers 4-1 to 4-W is considered. The number of types of transposition at this time is as follows.

Specifically, when random transposition of q-valued random numbers is performed at the average width W, the number of types of transposition is W!. At this time, because information carried by a q-valued W-digit number is q^W, it is found that transposition rule cannot be uniquely determined from the obtained random numbers if $W! > q^W$. When logarithm is applied to the above inequality,

$$W \log q < \log W! \fallingdotseq W \log W/e$$

is obtained. Therefore, if $W > q*e$, the above inequality is satisfied. In other words, even if the random number generating algorithm is known, it is not possible to determine, from the obtained random numbers, which part of the random number series is used. This makes a random number unable to be analyzed.

(Embodiment)

Fig. 2 shows one embodiment of the present invention. In Fig. 2, numerals 1, 2, 3 and 4 correspond to those in Fig. 1, and numerals 5 and 6 denote AND circuits, respectively and numeral 7 denotes an OR circuit.

The shown structure represents the case of q=2, in which $W > 2*2.7$ is obtained from the above description and therefore W=8 is considered. In the drawing, one of eight buffers 4-1 to 4-8, for example, is selected by the output from the random number generator 1, and the output from the random number generator 2 is set to the selected buffer and simultaneously the value of the buffer is output.

It is possible to prevent the problems occurring at the initial stage by filling the eight buffers with random numbers at the start point or by discarding the certain number of output random numbers which are first generated.

In the case of the shown embodiment, 3-bit information is discarded in order to obtain 1-bit output, and the discarded information cannot be reproduced from the obtained information. However, in practical use, it is sufficient to have four buffers. Further, it is also possible to eliminate one of the shown random number generators and to alternately extract an output from a single random number generator, for example, for generating first and second series of random sequences.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－246787

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開 昭和61年(1986)11月4日
G 09 C 1/00		7368－5B	

審査請求 有　発明の数 1　（全3頁）

㊹発明の名称　乱数混合処理方式

㉑特　願　昭60－63079
㉒出　願　昭60(1985)3月27日

㉒発明者　大磯　充夫　川崎市中原区上小田中1015番地　富士通株式会社内
㉑出願人　富士通株式会社　川崎市中原区上小田中1015番地
㉔代理人　弁理士 森田　寛　外1名

明　細　書

1．発明の名称　乱数混合処理方式

2．特許請求の範囲

（1）乱数発生器を有し，当該乱数発生器が発生する乱数を混合して使用する乱数生成方式において，1つまたは複数個の乱数発生器（1および／または2）とW個のバッファとをそなえ，

上記乱数発生器から出力される第1系列の乱数列の夫々の値にもとづいて上記W個のバッファのいずれか1つを選択すると共に，

上記乱数発生器から出力される第2系列の乱数列の夫々の値を，上記選択された1つのバッファに格納し，かつ当該バッファから格納されている内容を出力するよう構成した

ことを特徴とする乱数混合処理方式。

（2）上記W個のバッファは，上記第2系列の乱数列がq進の乱数で与えられるとき，実用上，

$W \geq 2.73 * q$

の個数をもつことを特徴とする特許請求の範囲第（1）項記載の乱数混合処理方式。

3．発明の詳細な説明

〔概要〕

乱数発生器からの出力を混合して使用する乱数生成方式において，W個のバッファのうちのいずれに格納しかつ出力するかを，他の乱数列にて決定するようにし，上記W個の個数を所定個数以上に選んで，解読を実用上不可能な乱数を生成することが開示されている。

〔産業上の利用分野〕

本発明は，乱数混合処理方式，特に乱数発生器から出力される乱数列を，実用上解読不可能な乱数を得るように，混合する乱数混合処理方式に関するものである。

〔従来の技術〕

乱数式暗号の強度は乱数の解析強度により定ま

る．乱数の発生方式は数理科学№203(May1980) p77にあるように多くの方式がある．解析強度からは自然乱数が理想的であるが，実用上は連鎖乱数を採用せざるを得ない．連鎖乱数には中央2乗法，混合合同法，フィード・バック・シフト・レジスタなどがある．このまま使用したのでは容易に乱数発生アルゴリズムを解析されるので一般に圧縮変換などを施して使用する．この乱数混合方式の1つとして前に特願昭58－19422号（乱数混合回路）を発明した．

〔発明が解決しようとする問題点〕

上記特願昭58－19422号に開示される乱数混合回路においては，乱数発生器から出力される乱数列について，圧縮変換および／または転置を行って実用上，解読不可能な形で乱数を生成することを示した．

しかし，上記特願昭58－19422号に示した構成を考慮しつつ，q進の乱数を平均幅Wにて乱転置することを考慮したとき，上記平均幅Wが十分に大であれば，実用上，解読不可能な乱数を得ることが可能であることが見出された．

〔問題点を解決するための手段〕

第1図は本発明の原理ブロック図を示している．図中の符号1は第1の乱数発生器，2は第2の乱数発生器，3はデコーダであってW個存在するバッファのうちのいずれか1つを選択するもの，4－1ないし4－Wは夫々バッファであって，第2系列の乱数列の各値を上記デコーダ3からの指示によって格納しかつ出力するものを表わしている．

〔作用〕

第1図において，図示第2の系列の乱数列がq進の乱数であるとして，それをW個のバッファ4－1ないし4－Wにランダムに分配する乱転置を考える．そしてこのときの転置の種類数を考えると次の如くなる．

即ち，q進の乱数を平均幅Wにて乱転置するとき，転置の種類数はW！となる．このときq進W桁の数の持つ情報はq^WであるのでW！＞q^Wとなれば，入手した乱数からは転置規約を一義的に決定できなくなることが判る．この不等式の対数をとって

$$W \log q < \log W! \fallingdotseq W \log W / e$$

であるからW＞q＊eであれば上記不等式が成立する．つまり，乱数発生アルゴリズムを知っていても，入手した乱数からは乱数系列のどの部分を使用したか決定できない．これは解析不能なる乱数である．

〔実施例〕

第2図は本発明の一実施例を示し，図中の符号1，2，3，4は第1図に対応し，5および6は夫々アンド回路，7はオア回路を表わしている．

図示の構成は，q＝2の場合を表わしており，上記の説明からW＞2＊2.7であり，W＝8を考えればよい．図において，乱数発生器1の出力により，例えば8個のバッファ4－1ないし4－8のうちの1個を選択し，当該バッファに乱数発生器2の出力をセットすると同時に，そのバッファの値を出力する．

スタート時点にて8個のバッファに乱数を満たしておくかとか，最初に発生した何個かの出力乱数を捨てることにより，初期時における問題を回避することができる．

図示実施例の場合には，1ビットの出力を得るために3ビットの情報を捨てており，得られた情報から捨てた情報を再現する事はできない．しかし，実用上は4個のバッファをもつだけでも十分である．また，図示の乱数発生器の一方を削除し，1つの乱数発生器からの出力を例えば交互に抽出して，第1系列と第2系列の乱数列をつくることもできる．

〔発明の効果〕

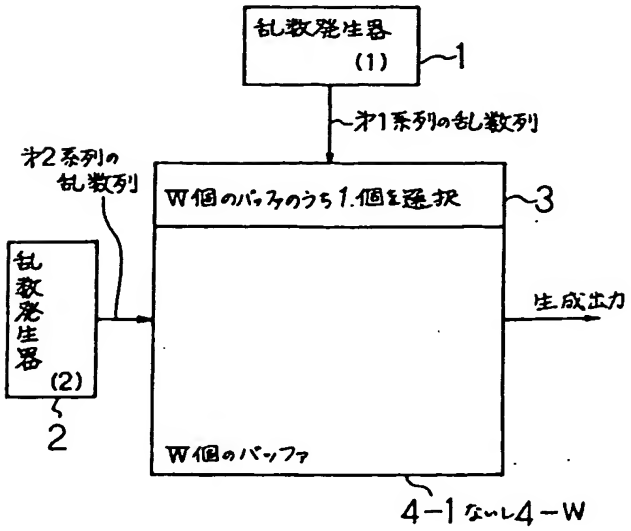
以上説明した如く，本発明によれば，比較的簡単な構成によって，実用上，解読不可能な暗号を生成することができる．

4．図面の簡単な説明

第1図は本発明の原理ブロック図，第2図は本発明の一実施例構成を示す。

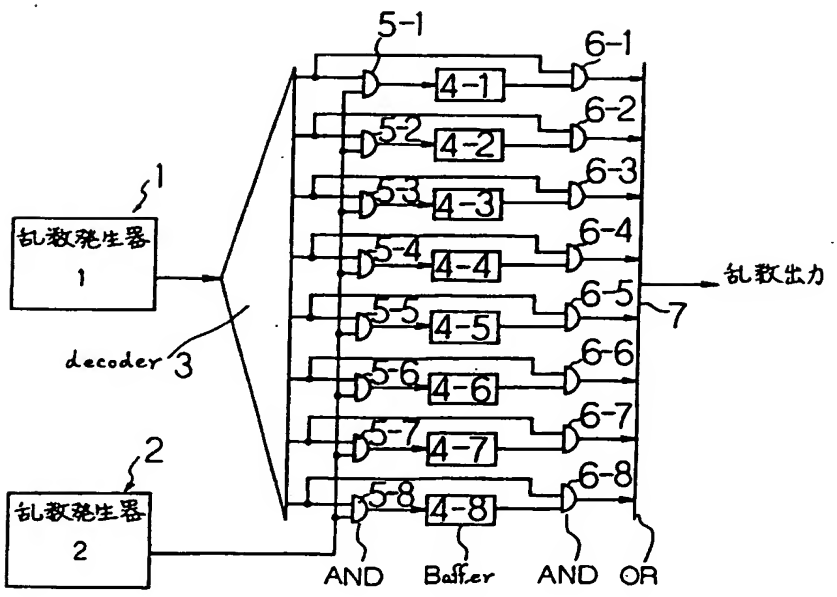
図中，1，2は夫々乱数発生器，3はデコーダ，4－1ないし4－8は夫々バッファ，5－1ないし5－8と6－1ないし6－8とは夫々アンド回路，7はオア回路を表わす。

特許出願人　　富士通株式会社
代理人弁理士　　森田　寛（外1名）



本発明の原理ブロック図

第1図



本発明の一実施例

第2図